AMENDMENTS TO THE CLAIMS

The following is a complete listing of revised claims with a status identifier in parenthesis.

LISTING OF CLAIMS

1.   (Currently Amended) An electronic data processing method method wherein users are assigned a data key the method comprising:

performing a security check to ascertain [[an]] a user identity of a user by comparing entered identity information with stored user identity data;

associating the user identity with a user identifier;

associating the user identifier with at least one user group identifier;

group including a plurality of users such that a data key is assigned to the user based on the user group with which the user is associated,

selecting a user group identifier and acquiring at least one data key associated therewith from a centralized data store including all available keys, at least one user group identifier and at least one data key being associated with one another;

the data key being unviewable by the user, and the data key being for performing at least one of encrypting and decrypting data using the acquired at least one data key and inhibiting user recognition of the acquired at least one data key, the same data key being assignable to the plurality of users.

2.   (Currently Amended) The method as claimed in claim 1, wherein the security check involves at least one of checking a user-specific biometric data, an electronic key and a mechanical key of the user.

3. – 4. (Canceled)

5.   (Currently Amended) The ~~method~~ <u>system</u> as claimed in claim [[4]] <u>8</u>, wherein ~~the data obtained in the security check are compared with the content of~~ the data key ~~memory~~ <u>is accessible</u> using a data telecommunication device.

6.   (Currently Amended) The method as claimed in claim 1, wherein a plurality of data keys are simultaneously assignable to one user <u>identifier</u>.

7.   (Currently Amended) The method as claimed in claim 1, wherein the data are medically relevant, wherein the users include personnel [[at]] <u>within</u> a medical facility, and wherein common user ~~groups~~ <u>group identifiers</u> are assigned the same data key.

8.   (Currently Amended) An electronic data processing <u>system</u> ~~facility~~ comprising:

        <u>a</u> security check <u>device</u> ~~means for performing a security check~~ to ascertain <u>user identity</u> ~~an identity of the user~~;

        ~~means for associating the user with a user group including a plurality of users~~<u>a first data store for storage and retrieval of at least one user identifier and associated user identity data;</u>

        <u>a second data store for storage and retrieval of the at least one user identifier and associated at least one user group identifier;</u>

a centralized third data store for storage and retrieval of all available data keys, the centralized third data store including at least one associated user group identifier matched with at least one associated data key; and

at least one processor to ascertain a user identifier by comparing data between the security check device and the first data store, to ascertain at least one user group from the second data store, to ascertain at least one data key for at least one user group from the third data store, and for performing at least one of data encryption and decryption using the at least one data key.

~~, the user being associated with the user group such that a data key is assigned to the user based on the user group with which the user is associated, the data key being unviewable by the user, and the data key being for at least one of encrypting and decrypting data, the same data key being assignable to various the plurality of users.~~

9.   (Currently Amended) The electronic data processing <u>system</u> ~~facility~~ as claimed in claim 8, wherein the security check <u>device reads</u> ~~means is for checking~~ biometric data from the user.

10.   (Currently Amended) The electronic data processing <u>system</u> ~~facility~~ as claimed in claim 8, wherein the security check <u>device</u> ~~means is for checking~~ <u>is</u> a user-specific at least one of electronic and mechanical key.

11.   (Canceled).

12.   (Currently Amended) The electronic data processing <u>system</u> ~~facility~~ as claimed in claim 11, ~~wherein the data key memory is arranged remotely from the data processing facility, and~~ wherein the ~~data processing~~ <u>system</u> ~~facility~~ uses a data telecommunication device to access the <u>third data store</u> ~~data key memory~~.

13.   (Currently Amended) The electronic data processing <u>system</u> ~~facility~~ as claimed in claim 8, wherein the ~~data processing~~ <u>system</u> ~~facility~~ is a medical workstation for handling medically relevant data.

14.   (Currently Amended) A <u>computer-readable</u> storage medium <u>including computer executable instructions that, when executed, cause a computer to</u> ~~, adapted to store information and adapted to interact with a data processing facility in order to~~ carry out the method as claimed in claim 1.

15. - 21.   (Canceled).

22.   (Previously Presented) A method for at least one of encryption and decryption of data, comprising:

performing a security check to ascertain an identity of a user;

associating the user with a user group including a plurality of users such that a data key for at least one of encrypting and decrypting data is assigned to the user based on the group with which the user is associated, the same data key being assignable to the plurality of users; and

at least one of encrypting or decrypting data using the assigned data key.

23.   (Currently Amended) A <u>computer-readable</u> storage medium <u>including computer</u> <u>executable instructions that, when executed, cause a computer to,</u> ~~adapted to~~ ~~store information and adapted to interact with a data processing facility in~~ ~~order to~~ carry out the method as claimed in claim 22.

24.   (Original) The method as claimed in claim 22, wherein the security check involves checking biometric data of the user.

25.   (Original) The method as claimed in claim 22, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

26.   (Original) The method as claimed in claim 22, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

27.   (Original) The method as claimed in claim 26, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

28.   (Original) The method as claimed in claim 22, wherein a plurality of data keys are simultaneously assignable to one user.

29.   (Original) The method as claimed in claim 22, wherein the data are medically relevant, wherein the users include personnel at a medical facility, and wherein common user groups are assigned the same data key.

30.   (Original) The method of claim 22, wherein users associated with a common user group are assigned the same data key.

31.   (Previously Presented) An electronic data processing facility for at least one of encryption and decryption of data, comprising:

        means for performing a security check to ascertain an identity of a user;

        means for associating the user with a user group including a plurality of users a data key is assigned to the user based on the group with which the user is associated, the same data key being assignable to the plurality of users, and the data key being for at least one of encrypting and decrypting data; and

        means for encrypting or decrypting data using the assigned data key.

32.   (Currently Amended) The method of claim 1, wherein <u>a user identifier</u> ~~users~~ associated with a common user group <u>identifier</u> [[are]] <u>is</u> assigned the same data key.

33.   (New) The system of claim 8, further comprising:

        A fourth data store for storage and retrieval of encrypted data.

34.   (New) The system of claim 8, wherein at least one of the first data store, the second data store and the fourth data store are combined.

35. (New) The system of claim 8, wherein the data store comprises:

mechanical memory, electronic memory, and magnetic and optical media data

storage.

36. (New) The system of claim 8, wherein the third data store is isolated from the

first, second and fourth data stores.

37. (New) The system of claim 8, wherein data entry and retrieval is at least one of

manual and automated.

38. (New) The system of claim 12, wherein the data telecommunications device is

removably and operatively associated with a computer network for transfer of data.

39. (New) The system of claim 8, wherein the channel comprises an access and

restriction process.

40. (New) The system of claim 39, wherein the channel access and restriction

process functions operatively with the security check device.